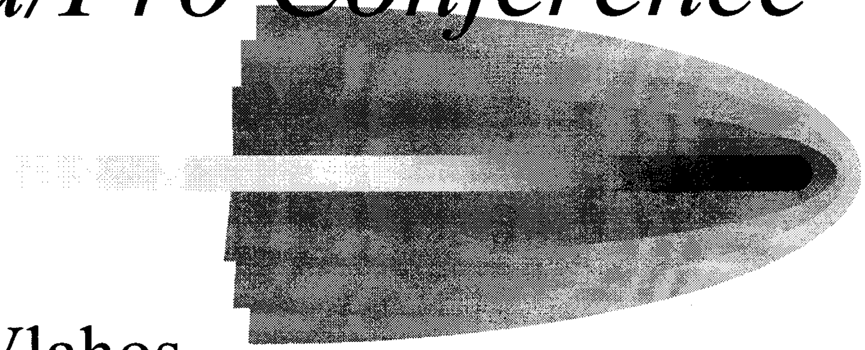
# *Virtual Private Networks (VPN)*
# *Next Generation Remote Access*
# *MacWorld/Pro Conference*



Bill Vlahos

Network Services Engineer

OAO Corporation contracted to Jet Propulsion Laboratory

January 6, 2000

# *Objectives*

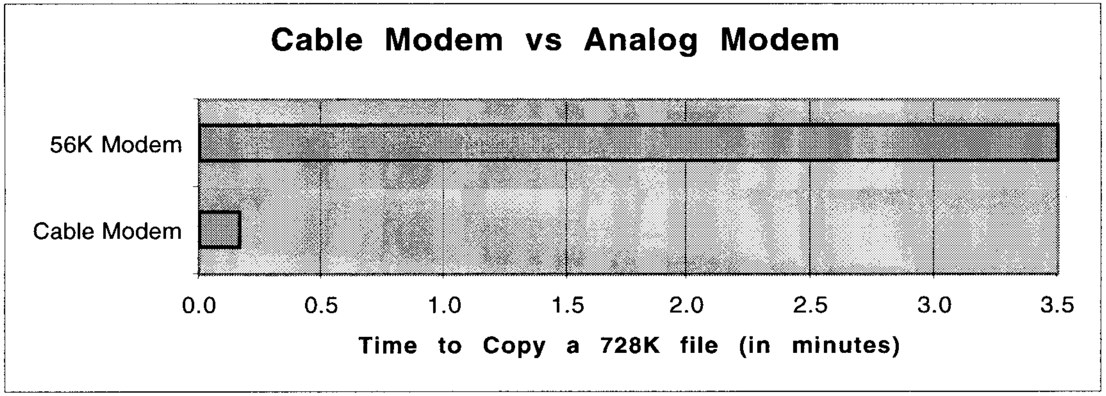
- What is Remote Access?
- What is a VPN?
- Why do I want it?
- How do I choose it?
- Is it ready to use now?
- Opportunities to lead using Macs
  - Most common VPN is Microsoft’s built-in

# *Introduction to Remote Access*

- Current situation
  - Dial up 56k v.90 or 128k ISDN
    - Multi-protocol
  - IP via Internet
    - IP only
    - IP address restriction on web & ftp servers
    - Clear text with little encryption

# *Technology Direction*

- High speed, secure access from anywhere changes the whole notion of accessing corporate networks. Cable modems and DSL gives us capabilities not practical with even the fastest analog or ISDN modems.
- Virtual Private Network technologies give Network Administrators the opportunities to be *heroes* by providing high speed connectivity with secure and controlled access to corporate networks.
- The technology works and it's not even very expensive.



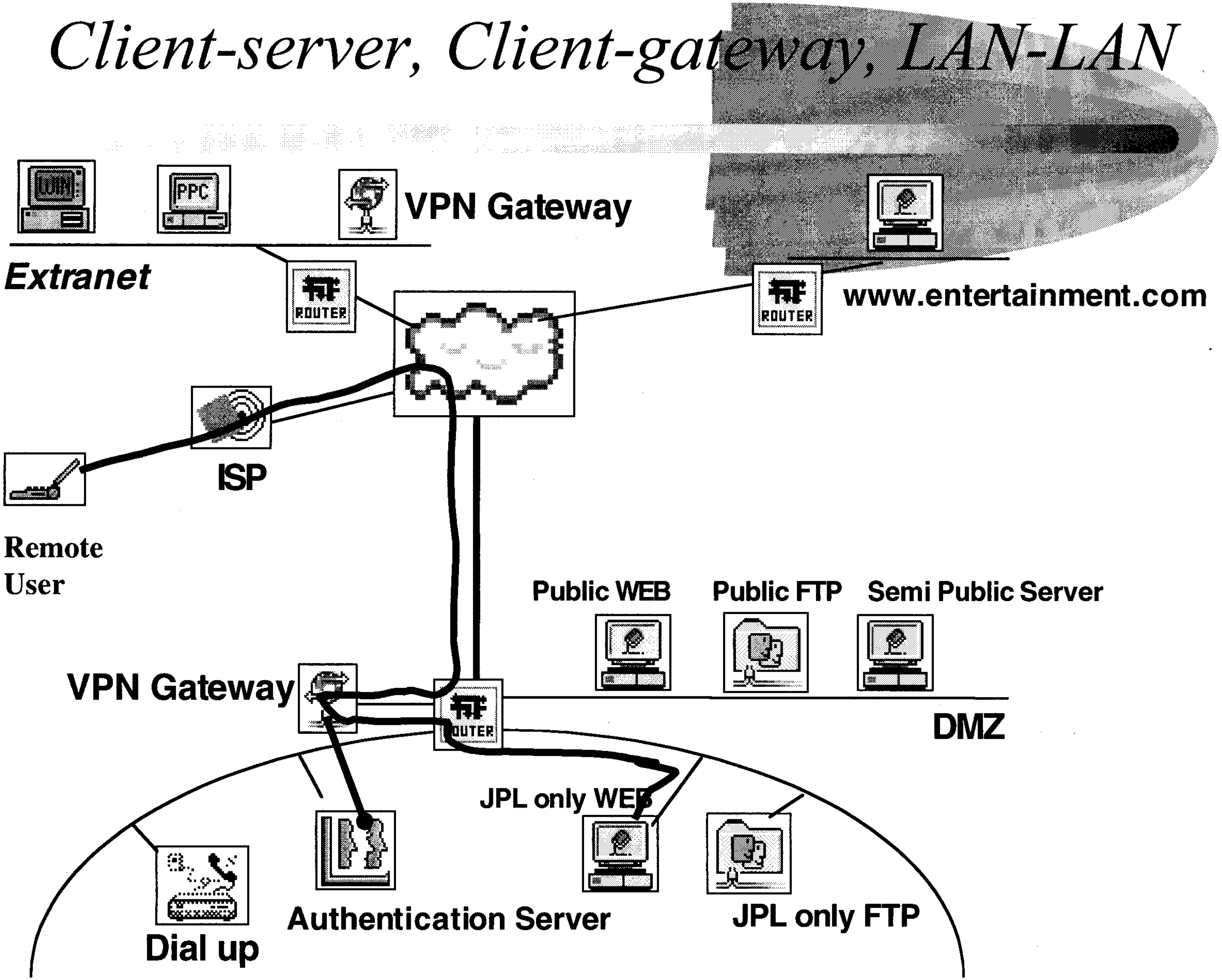
# *What is a VPN?*

**High-speed, secure, controlled connections from anywhere!**

- Three forms
  - Client to server
    - Software solution plus authentication (often local)
  - Client to network (gateway)
    - Client software gateway software or hardware plus authentication server
  - Network to network (Gateway-gateway or LAN-LAN)
    - Hardware solution for stability and performance

# *VPN Design Overview*

## *Client-server, Client-gateway, LAN-LAN*



# *Which type of VPN?*

- Client-server
  - Complete encryption end to end
  - Doesn’t scale easily/how do you authenticate users
  - Performance and security issues
- Client-network
  - High performance
  - Scalable (can leverage existing infrastructure)
  - Requires client software
- Network-network
  - No client requirements (support all platforms)
  - Doesn’t go everywhere

# *The 3 Components of a VPN Focus on Client-network*

- VPN Gateway
  - External interface(s) (IPSec only)
  - Internal interface(s) (inside Company network)
    - May be multi-protocol
- Authentication Server
- Client software

# Features & Options

- Authentication Servers
  - RADIUS
  - SecureID Card
  - PKI
- Type of Gateway
  - Appliance Box
  - Software application
- Performance Expectations
  - Simultaneous connections
  - Network throughput
- Standards
  - PPTP (Microsoft)
  - L2TP (Microsoft & Cisco)
  - IPSec (Ratified standard)
- Services
  - IP
  - AppleTalk
  - IPX
  - NAT (Network Address Translation)
  - Encryption levels (DES, 3DES, etc)

# Macintosh Supported Vendors

| Vendor (Alphabetical) | IPSec | RADIUS | Form | Notes |
|---|---|---|---|---|
| Raptor VPN/Axent | No | No | S/W | Formerly AltaVista Tunnel-Compaq |
| Bay Networks/Nortel | No* | Yes | Box | Uses NTS client, Mac IPSec soon |
| Cisco Systems | Yes | No | Both | Can use PGPNet client |
| Compatible Systems | Yes | Yes | Box | Client software FREE |
| InfoExpress | No | Yes | S/W | Proprietary standard |
| iPass | No | No | N/A | iPass dialup private network |
| Microsoft | No | No | S/W | Can use NTS client |
| Network Associates(PGPnet) | Yes | No | S/W | Point-point & point-gateway |
| PGPnet from MIT (Freeware) | Yes | No | S/W | Point-point build your own |
| Network TeleSystems(NTS) | No | Yes | Both | PPTP only |
| TimeStep | Yes | No* | Box | |
| V-ONE | No | Yes | S/W | |

**Promised in future by vendor*

# *Contacting Vendors*

AltaVista Tunnel /Compaq http://altavista.software.digital.com/tunnel/

sold to Axent http://www.axent.com (Raptor Mobil-EC)

Bay Networks/Nortel http://www.nortelnetworks.com

Cisco Systems http://www.cisco.com

Compatible Systems http://www.compatible.com

InfoExpress http://www.infoexpress.com

*iPass http://www.centralhouse.com/ipass/service_overview.html

Network Associates(PGPnet) http://www.nai.com/

PGPnet from MIT (Freeware) http://web.mit.edu/network/pgp.html

Network TeleSystems(NTS) http://www.nts.com/

TimeStep http://www.timestep.com

V-ONE http://www.v-one.com/smartgate.htm

# *Authentication Servers*

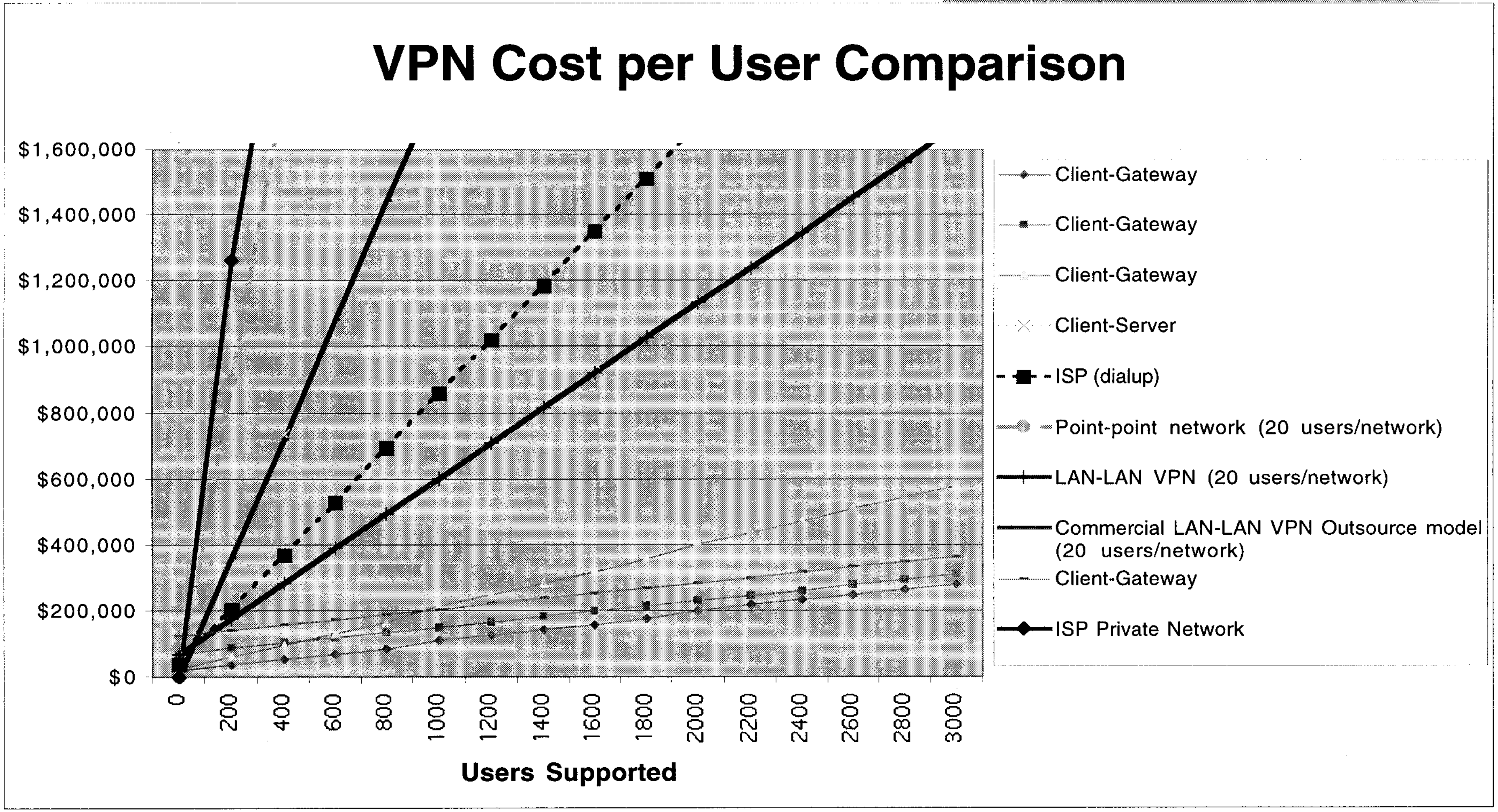
- MacRADIUS http://www.cyno.com
  - IETF Standards based RADIUS (Remote Authentication Dial-in User Service) server with extensive AppleScript support.
- Accounts on the Gateway
  - Not scalable
- Public Key Infrastructure (PKI) - not Mac based
  - Entust http://www.entrust.com/
  - Versign http://www.verisign.com/
  - x.509 Certificates

# *Sample Requirements for VPNs*

## *your mileage may vary*

- **Encryption (IPSec)**
- **smart tunnel (appropriate use)**
- **NAT (Network Address Translation)**
- **log source and NAT IP addresses**
- log traffic indicator
- **RADIUS**
- IKE/PKI Entrust (in future)
- Y2K
- Encryption key rotation
- IP
- AppleTalk
- IPX
- failover & redundancy
- Connectivity (Client-gateway, gateway-gateway, gateway at edge of JPL network)
- **Mac**, Win95/98/NT
- **client s/w exportable**
- **application independent**
- 500 simultaneous connections
- 27 Mb/s throughput
- load balancing
- password protected
- Console port protected
- passwords changeable
- SNMP monitoring
- vendor replacement

# *Cost per user for 3 years*



# *Client-Gateway VPN*

- Advantages
  - All network services automatically protected
  - Ubiquitous Internet access
  - ISP & technology independent
  - Traffic is encrypted before it leaves computer
  - User is authenticated at connection time
  - Smart tunnel feature assures “appropriate usage”
  - Standards based (IPSec)
  - Leverage current infrastructure (authentication, etc.)
  - No changes to existing services
- Disadvantages
  - Software installed on remote client computer

# *Gateway-Gateway VPN*

- Advantages
  - Does not require client installs on remote computers
  - Supports all computer platforms
  - ISP independent. Gateway(s) can be anywhere on the Internet
  - Smart tunnel feature assures “appropriate usage”
  - “Always-on” connection
- Disadvantages
  - Difficult to control who is on the remote network

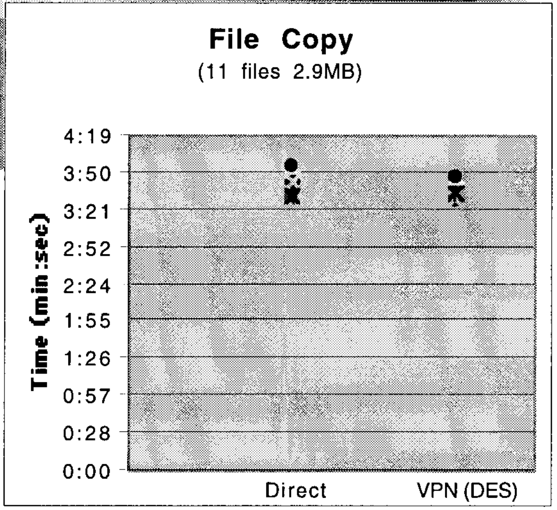
# *So does it work?*

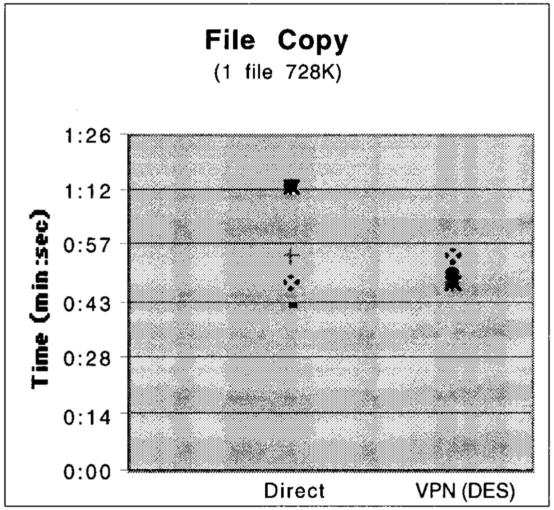
- Yes!

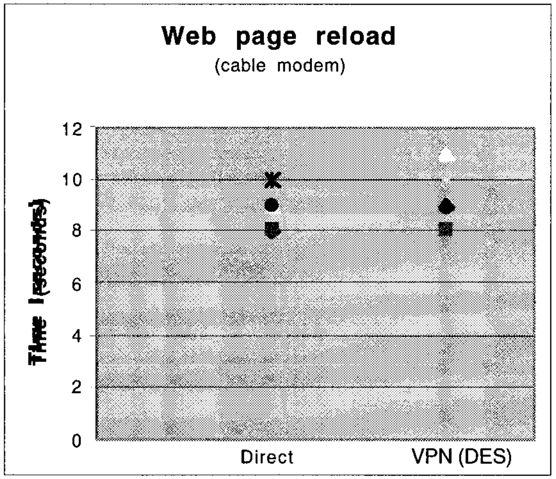
- How well do you ask?...

# *VPN Performance Impact High-speed cable modem*

- **We expected to see some degradation but did not find any.**



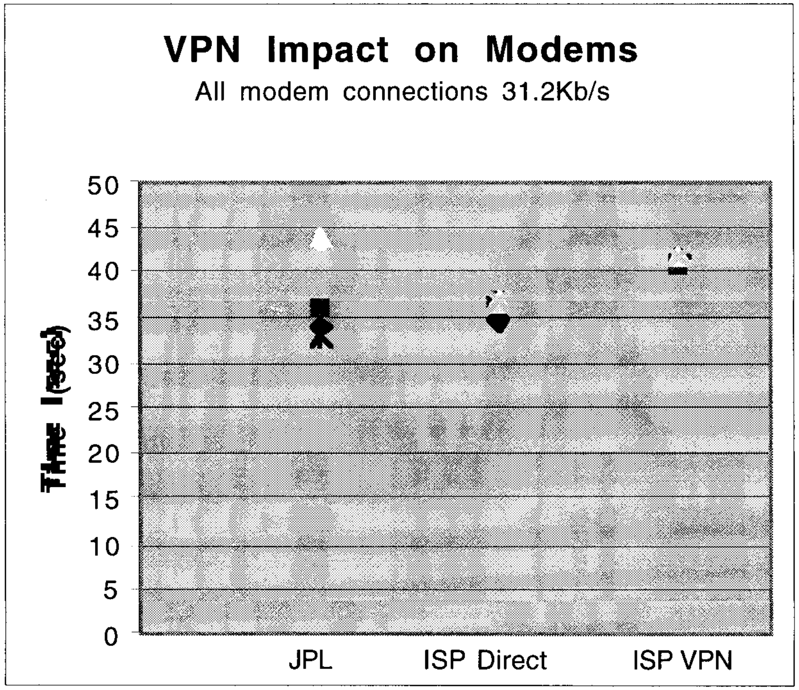


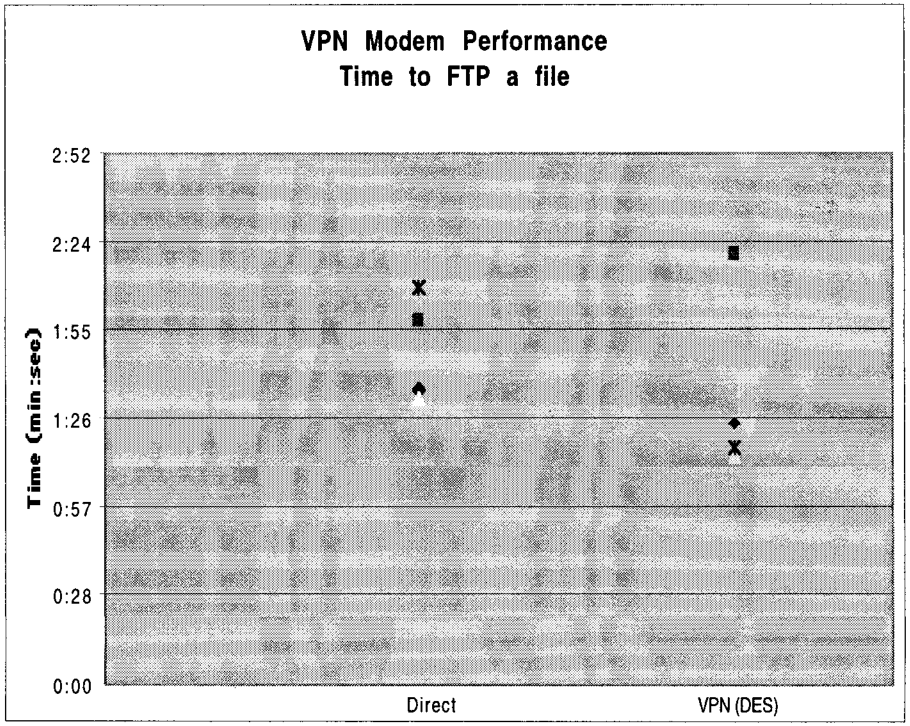


# *VPN Performance Impact*
# *Analog Modems*

- **Good line conditions**
  **Small penalty (17%)**

- **Poor line conditions**
  **No consistent penalty**

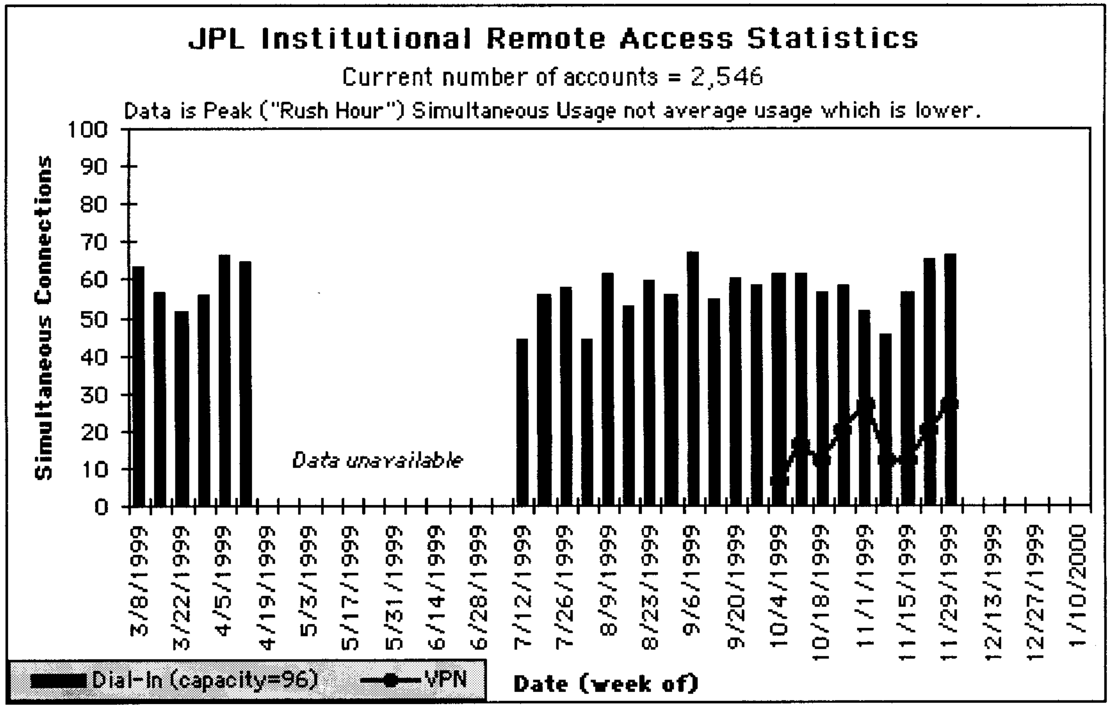




# *Case Study*
# *JPL's Deployment Story*

Two (2) Months Ago

- Instructions on WEB
- Software on JPL WEB
  - 1,750 accesses
- 600 client downloads
- 400 different users
- <50 HelpDesk calls



# *Challenges for deployment*

- Remote site firewalls
  - Corporate configuration and policies
  - Personal (Macintouch has great report)
    - http://www.macintouch.com/accessrouters.html
- Support of computers owned by other institutions
- Who will support outside users
- Export controls on encryption software (US Gov.)
- IPSec ratified Nov. ‘98. Will take time to stabilize
- Cross-vendor compatibility not good

# *Risks of VPNs*

- Cable modems and DSL are "Always ON"
  - If they become compromised while a tunnel is up, the intruder has access to VPN network.
  - Protect w/personal firewalls
    - Macs are better protected than other platforms
  - Adjust or eliminate "Smart Tunnel" feature
- Password security
  - Embedded passwords?
  - Make sure password transit is encrypted too.

# *Additional Information*

- IPSecurity (IPSec) RFC 2409 (IKE {Internet Key Exchange}) and RFC 2407 (ISAKMP {Internet Security Association and Key Management Protocol}). http://www.ietf.org/html.charters/ipsec-charter.html
- RADIUS (Remote Authentication Dial In User Service) RFC 2058 (Authentication) and RFC 2059 (Accounting)
- My email address: bvlahos@jpl.nasa.gov

*Demo*

# Q & A

*Thank you*